NEW ZEALAND DIGITAL IDENTITY – ACCOUNTABILITY AND ARCHITECTURE MAP

Who holds decision rights, what the legal framework is, and where responsibility sits

Public-source record | July 2026

1. Purpose

This note maps the current official structure of New Zealand's digital identity system for public-interest accountability purposes. It identifies the legislation, the Minister and agencies with decision rights, the regulator, the main operational systems (including biometric use), and the principal international standards that the framework aligns with. It is based solely on published government sources as at July 2026.

2. Core Legislation

• Digital Identity Services Trust Framework Act 2023 – primary statute establishing the legal framework for accredited digital identity services, the Trust Framework Authority, and the Trust Framework Board.

• Digital Identity Services Trust Framework Regulations 2024 (as amended 2026) – accreditation process, service types, and related requirements. Administered by the Department of Internal Affairs.

• Digital Identity Services Trust Framework Rules 2024 (as amended 2025-1 and 2026-1) – technical and operational requirements for accredited providers. Latest consolidated version comes into force 29 June 2026. Amendment Rules 2026-1 were signed by the Minister for the Public Service and Digitising Government.

• Electronic Identity Verification Act 2012 – governs RealMe verified identity (electronic identity credentials). Separate from but related to the Trust Framework.

3. Current Ministerial and Agency Responsibility

3.1 Minister

Hon Paul Goldsmith, Minister for the Public Service and Digitising Government, is the Minister responsible for the Digital Identity Services Trust Framework Act 2023. He signed the Digital Identity Services Trust Framework Amendment Rules 2026-1 (Gazette notice 29 May 2026; in force 29 June 2026).

3.2 Agencies and bodies

• Government Digital Delivery Agency (GDDA) – established within the Public Service Commission from 1 April 2026 when GCDO functions transferred from DIA. Hosts the Trust Framework Authority. Responsible for the Digitising Government work programme, including accelerating trusted digital identity and a credential issuance platform (live end of March 2026).

• Trust Framework Authority – statutory regulator of accredited digital identity services. Accredits providers and services, handles complaints and non-compliance. Contact domain under GDDA.

• Trust Framework Board – recommends amendments to the Rules to the Minister under section 18 of the Act.

• Department of Internal Affairs (DIA) – continues to administer the Regulations; operates RealMe and the Identity Verification Service under the Electronic Identity Verification Act;

historically led much of the policy development. Secretary for Internal Affairs has publicly spoken on rule updates.

• Public Service Commission – parent body for GDDA from April 2026.

4. Operational Systems and Biometric Use

• RealMe verified identity – government-issued digital identity linked to a RealMe login. Includes a photograph. Facial recognition technology is used by DIA to verify identity and check against other identity records (verified identities and New Zealand passports). Photographs are stored for future matching. Retention periods are set in legislation (verified identity and photograph held for 11 years from cancellation or expiry in relevant cases).

• Digital credentials / wallets – under the Trust Framework, accredited credentials (including government-issued such as driver licences and other attributes) can be held in digital wallets. Official material states credentials remain encrypted on the user's device and that the Trust Framework does not create a central database or track users. Device biometrics (fingerprint / facial recognition) are used to protect access to the wallet in the Govt.nz app context.

• AML Identity Verification Code of Practice 2026 (effective July 2026) – updates anti-money laundering identity verification rules to support reusable digital identity and accredited electronic verification services, creating a clearer pathway for wider private-sector use of accredited digital credentials and biometric verification.

5. Official Stated Design Features

Published government material consistently states that:

• Use of digital identity services is optional.

• The Trust Framework does not create a central database or track users.

• Organisations cannot exchange user information without consent under the Framework design.

• Accredited digital wallets keep credentials encrypted on the user's device; issuers do not have visibility when a credential is presented.

These are the official design claims. Accountability documentation should record both the claims and any later divergence from them.

6. International Alignment and Standards Influence

New Zealand's framework is explicitly developed "in line with international standards and best practice." The main reference points visible in public material include:

• W3C Verifiable Credentials and related emerging standards for interoperable credential presentation (referenced in the 2026 Rules amendments).

• Identification and assurance standards used for independent evaluation of services.

• Comparable programmes in other jurisdictions (Australia's digital identity work, EU eIDAS / European Digital Identity Wallet direction, and similar reusable-credential models) which supply both technical patterns and policy language.

Global technology vendors and standards bodies shape the available tooling and the default architectures that national frameworks adopt. Decision rights for New Zealand's legal design and accreditation rules remain with the New Zealand Minister, GDDA/Trust Framework Authority, DIA, and Cabinet as applicable.

7. What is Already Documented vs What May Still Require Official Information

Already on the public record (and summarised here): the Act, Regulations, Rules and amendments; ministerial responsibility; agency transfer of GCDO functions to GDDA; existence of the Trust Framework Authority and Board; RealMe biometric facial matching practice; AML Code of Practice shift toward reusable digital ID; official design claims (optional, no central database, on-device credentials).

Areas that may still justify targeted Official Information Act requests if deeper accountability is required:

• Specific risk assessments or advice on permanence of biometric identifiers, breach consequences, and function-creep scenarios provided to Ministers or the Trust Framework Board.

• Cabinet or ministerial papers that set the policy direction for accelerating digital identity and credential issuance.

• Any internal assessments of residual risk remaining after the “no central database / on-device” design claims.

• Cost, uptake, and private-sector reliance assumptions underpinning the AML and Trust Framework rollout.

Broad new OIAs are not the first step. The public architecture is already clear enough to map responsibility. Targeted requests should be reserved for specific risk or decision documents that are not already published.

8. Accountability Use of This Map

This document is intended as a dated public-source baseline. When systems expand, when biometric data is compromised, or when optional systems become effectively mandatory in practice, the record of who held the decision rights, what the stated design was, and what risks were knowable at the time is the basis for accountability. Names of public office-holders and published institutional roles are fair subjects of such a record. Private individuals without decision rights are not.

9. Primary Public Sources (July 2026)

• Digital Identity Services Trust Framework Act 2023; Regulations 2024 and Amendment Regulations 2026; Rules 2024 and Amendment Rules 2025-1 / 2026-1 (Gazette and legislation sites).

• Briefing to the Incoming Minister for Public Service and Digitising Government, April 2026 (Public Service Commission / GDDA).

• DIA and GDDA Trust Framework web pages; RealMe Identity Verification Service privacy material.

• AML Identity Verification Code of Practice 2026 reporting and related ministerial statements.

• Govt.nz app support material on digital identity credentials and device biometrics.

Public-interest accountability map prepared from published government sources only. July 2026.